

### REMARKS

In the Office Action dated December 14, 2004, claims 41-43 were rejected under 35 U.S.C. § 112, ¶ 1; claims 2, 3, 6-8, 12, 13, 19, 21-23, 28, 30, and 32-39 were rejected under § 102 over U.S. Patent No. 6,473,798 (Grosser); claims 4, 5, 16, 17, 20, and 41-43 were rejected under § 103 over Grosser in view of U.S. Patent No. 6,182,226 (Reid); claims 9, 10, 24, 25, and 29 were rejected under § 103 over Grosser in view of U.S. Patent No. 6,636,898 (Ludovici); and claim 26 was rejected under § 103 over Grosser in view of U.S. Patent No. 6,173,411 (Hirst).

Claims 3, 19, 23, 33, 36, and 40-43 have been cancelled, without prejudice, to render the rejection of those claims moot.

Amended independent claim 32 is not anticipated by Grosser. Claim 32 recites a method comprising:

- establishing a secure link between a first node and second node according to an IPsec protocol;
- sending at least one ping message targeting the second node over the security link, the at least one ping message defined outside the IPsec protocol; and
- monitoring for at least one ping reply to *determine if an IPsec security association of the secure link is valid*,
- wherein sending the at least one ping message comprises sending the at least ping message *protected according to the IPsec protocol*.

It is respectfully submitted that Grosser does not teach monitoring for at least one ping reply to determine if an IPsec security association of the secure link is valid. The Layer 2 test packets sent in the system of Grosser is used to detect whether a Layer 2 tunnel is down. However, Grosser does not teach the monitoring for at least one ping reply to determine if an IPsec security association of a secure link is valid. There is no mention in Grosser of detecting for the validity of an IPsec security association.

Moreover, it is respectfully submitted that the Layer 2 test packet (L2TP Hello, L2F\_ECHO, or PTP Echo-Request) as taught by Grosser *is not protected according to an IPsec protocol*, as recited in claim 32.

Grosser focuses on testing a *Layer 2 tunnel* in a communications network. *See* Grosser 2:66-67 (“[T]he present invention provides a method and system for testing a Layer 2 tunnel.”).

As expressly taught by Grosser, “the three Layer 2 tunnels discussed above do not themselves specify or provide data security.” Grosser, 4:23-24. The Examiner relied upon the following teaching of Grosser as disclosing the protection of the Layer 2 test packet by a security protocol: “However, PPP or IPsec packet encryption can be utilized in conjunction with Layer 2 VPN tunneling to provide packet security at least between tunnel endpoints [Grosser, 4:25-28].” There is no specific teaching in this statement of Grosser that the Layer 2 test packets are encrypted or protected by IPsec. The Office Action stated that “Grosser does not state Layer 2 test packets would be excluded from protection if IPsec were used.” 12/14/2004 Office Action at 18. However, Applicant notes that Grosser does not teach that Layer 2 test packets are in fact protected by IPsec. The most that can be gleaned from the column 4, lines 25-28, passage of Grosser is that IPsec packet encryption can be utilized in conjunction with Layer 2 VPN tunneling to provide packet security at least between tunnel endpoints. There is no teaching that IPsec packet encryption can be applied to Layer 2 packets. The Office Action has pointed to no other passage of Grosser that would provide the requisite teaching that the Layer 2 test packets of Grosser are protected by IPsec.

The Office Action also pointed to sections 9.2 and 9.4 of RFC 2661 as supporting the rejection. 12/14/2004 Office Action at 18. Reliance on this secondary reference is improper, since the Office Action is rejecting the claim under § 102 not § 103. The Office Action has supplied no motivation for combining Grosser and RFC 2661. If the rejection is based on inherency, then the Office Action has failed to establish that the content of RFC 2661 is necessarily part of Grosser. *See* M.P.E.P. § 2112.

Moreover, section 9.2 of RFC 2661 teaches that securing L2TP requires that the *underlying transport* make available encryption, integrity and authentication services for all L2TP traffic. Section 9.4 of RFC 2661 teaches that IPsec provides packet-level security via ESP and/or AH, and that all L2TP controlling data packets for a particular tunnel appear as homogenous UDP/IP data packets to the IPsec system. As an initial note, there is no teaching whatsoever in RFC 2661 that Layer 2 test packets are encrypted or otherwise protected by IPsec. Moreover, it is noted that RFC 2661 specifically teaches that “[s]ecuring L2TP requires that the *underlying transport* make available encryption, integrity and authentication services for all L2TP traffic.” RFC 2661, at 69. Grosser specifically teaches that IPsec is implemented at Layer

3, whereas the Layer 2 tunneling protocols, such as L2TP, are implemented at Layer 2. Grosser, 1:61-65. By definition, Layer 3 is above Layer 2, and thus cannot be the *underlying transport* described in RFC 2661 on page 69 for securing L2TP. As is well known to persons of ordinary skill in the art, layer 3 information *passed down* to layer 2 is treated as data and encapsulated with layer 2 header and trailer information. See, e.g., "Introduction to Internet," at 7. Thus, a layer 2 packet contains the header, trailer, and data information of a layer 3 data unit. A Layer 3 protocol, such as IPsec, does not provide an underlying transport for a lower layer, Layer 2.

In view of the foregoing, the objective evidence establishes that a person of ordinary skill in the art would not understand Grosser as teaching the protection of Layer 2 test packets with IPsec. Therefore, it is respectfully submitted that Grosser does not anticipate claim 32.

Amended claim 38 is allowable for reasons similar to those of claim 32, since Grosser does not disclose monitoring for at least one ping reply to determine if a *security association* of the secure link is valid. Grosser also does not disclose sending a ping message protected according to a security protocol.

Amended independent claim 34 is also not disclosed by Grosser. Claim 34 recites establishing a secure link between a first security gateway and a second security gateway, where a remote node is in communication with the second security gateway over a network separate from the secure link. Also, the method of claim 34 includes sending at least one ping message to the remote node over the secure link, through the second security gateway, and over the network. The method further includes monitoring for at least one ping reply from the remote node to determine if the secure link is alive.

In Grosser, the Layer 2 test packets are not sent to a remote node that is in communication with a security gateway over a network separate from the secure link. As taught by Grosser, the Layer 2 tunnel can either be established between a network server 28 and a network access concentrator 20 (see Fig. 1), or between the network server 28 and a tunneling-enabled PPP client 52a or 52b. To understand the Layer 2 test packets, the receiving node in Grosser must *necessarily be tunneling-enabled*. Otherwise, the receiving node would not be able to receive the Layer 2 test packets. An example of this is shown in Fig. 1, where the Layer 2 tunnel is established between the access concentrator 20 and the network server 28, but not between the network server 28 and either the PPP client 26a or PPP client 26b, because the

PPP client 26a or 26b is not tunneling-enabled. In other words, the Layer 2 test packets *cannot* be sent beyond a tunneling-enabled node. Therefore, Grosser does not teach the sending of a ping message to a remote node over a secure link, through the second security gateway, and over the network, as recited in claim 34.

Claim 26 has been amended from dependent form to independent form, with its scope *unchanged*. Claim 26 was rejected as being obvious over Grosser and Hirst. The Office Action conceded that Grosser does not disclose establishing a link over a secondary communication network if the secure link is not alive. However, the Office Action cited Hirst as teaching the missing element. It is respectfully submitted that a *prima facie* case of obviousness has not been established with respect to claim 26, as no motivation or suggestion existed to combine the teachings of Grosser and Hirst. *See* M.P.E.P. § 2143 (8<sup>th</sup> ed., Rev. 2), at 2100-129.

The Office Action pointed to the passage of Grosser in column 5, at lines 9-12, as teaching the taking of remedial action. Note, however, that the remedial action referred to in the cited column 5 passage of Grosser is remedial action taken by *a network administrator*. Thus, what Grosser is teaching is that remedial action can be taken by a network administrator to correct problems with tunnel connectivity or responsiveness. There is no suggestion provided by Grosser in this passage of a system having a module to establish a link over a secondary communication network if the secure link is not alive.

Although Hirst teaches that the roles of primary and secondary connections are swapped if network connectivity is determined to be unacceptable, the teachings of Hirst are in an un-related context. Hirst does not provide any teaching or suggestion of testing a secure link using ping messages protected according to a security protocol.

A person of ordinary skill in the art looking at the disparate teachings of Grosser and Hirst would not have been motivated to combine the teachings of these references to achieve the claimed invention.

Therefore, a *prima facie* case of obviousness has not been established with respect to claim 26 over Grosser and Hirst.

Independent claim 5 was rejected as being obvious over Grosser and Reid. Claim 5 recites that sending the at least one ping message comprises sending at least one Internet Control Message Protocol message. The Office Action conceded that Grosser fails to disclose sending

an Internet control message protocol (ICMP) message as the ping message. 12/14/2004 Office Action at 9. However, the Office Action relied upon Reid as teaching this missing element. It is respectfully submitted that a *prima facie* case of obviousness has not been established with respect to claim 5, for at least the reason that the Office Action has failed to establish that there was any motivation or suggestion to combine the teachings of Grosser and Reid. The Office Action has also failed to establish that there would be any reasonable expectation of success in combining Grosser and Reid, which is another requirement of the *prima facie* case of obviousness. See M.P.E.P. § 2143 (8<sup>th</sup> ed., Rev. 2), at 2100-129.

There simply did not exist any reason to incorporate the teachings of Reid regarding ICMP ping messages into the Layer 2 tunnel testing mechanism of Grosser. As discussed above, the focus of Grosser is on testing Layer 2 tunnels with *Layer 2* test packets. Using a higher level ping message in place of the Layer 2 test packets would *render the Grosser mechanism inoperative for its intended purpose*. It is respectfully submitted that an ICMP ping message, as taught by Reid, cannot be used to test a Layer 2 tunnel, which is the focus of the teachings of Grosser. “If [a] proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.” M.P.E.P. § 2143.01, at 2100-131. The Office Action cited to no evidence that ICMP messages can be used to test a Layer 2 tunnel – yet, the Office Action stated that it would be reasonable to use an ICMP ping message to test connectivity and responsiveness of endpoints of a Layer 2 tunnel. 12/14/2004 Office Action at 21. Grosser is intended to detect whether a Layer 2 tunnel is down or not – using a higher level ICMP message would not achieve that purpose. More fundamentally, as Layer 2 test packets are available for testing Layer 2 tunnels, there would have been absolutely no reason whatsoever to employ a different level message, such as the ICMP ping message, to test the Layer 2 tunnels described in Grosser.

The Office Action has also failed to establish that there would have been a reasonable expectation of success in using the ICMP ping messages of Reid in testing Layer 2 tunnels of Grosser. See M.P.E.P. § 2143, at 2100-129 (“[T]here must be a reasonable expectation of success.”). It is highly unlikely that an ICMP message associated with a higher-level protocol can be used to successfully test a Layer 2 tunnel.

In response to Applicant's arguments that the Office Action has failed to establish that there would have been reasonable expectation of success, the Office Action asserted that the reasonable expectation of success requirement of a *prima facie* case of obviousness "deals with the Chemical and Biotechnology arts where there is an inherent level of unpredictability." 12/14/2004 Office Action at 22. The Office Action further stated that because the electrical and computer arts have a high level of predictability, that M.P.E.P. § 2143.02 states that "the burden is on the applicant to show evidence that there was no reasonable expectation of success." *Id.* at 22-23.

Applicant respectfully disagrees with this assessment. As expressly stated by M.P.E.P. § 2142, the "examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness." M.P.E.P. § 2142, at 2100-128. "If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness." *Id.* (emphasis added). The M.P.E.P. then lists the three elements of a *prima facie* case of obviousness: (1) there must be some suggestion or motivation to modify a reference or to combine reference teachings; (2) there must be a reasonable expectation of success; and (3) the prior art references when combined must teach or suggest all the claim limitations. M.P.E.P. § 2142, at 2100-128. There is no indication in the MPEP that the second requirement (that there must be a reasonable expectation of success) applies only to the chemical and biotechnology arts. In fact, it is respectfully submitted that § 2143.02 does not provide any statement that the burden is on applicant to show no reasonable expectation of success in the electrical and computer arts. It is therefore respectfully submitted that the Office Action has failed to satisfy the second requirement of a *prima facie* case of obviousness, namely that the Office Action has failed to establish that use of an ICMP ping message can be successfully used to test a Layer 2 tunnel.

In view of the foregoing, it is respectfully submitted that a *prima facie* case of obviousness has not been established with respect to claim 5.

Claim 20 is allowable over the asserted combination of Grosser and Reid for reasons similar to those given for claim 5.

Dependent claims are allowable for at least the same reasons as corresponding independent claims.

Appln. Serial No. 09/714,082  
Amendment Dated March 14, 2005  
Reply to Office Action Mailed December 14, 2004

In view of the foregoing, all claims are condition for allowance, which action is respectfully requested. The Commissioner is authorized to charge any additional fees and/or credit any overpayment to Deposit Account No. 20-1504 (NRB.0006US).

Respectfully submitted,

Date: March 14, 2005



---

Dan C. Hu  
Registration No. 40,025  
TROP, PRUNER & HU, P.C.  
8554 Katy Freeway, Suite 100  
Houston, TX 77024  
Telephone: (713) 468-8880  
Facsimile: (713) 468-8883